UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ARISTA RECORDS LLC, ATLANTIC RECORDING CORPORATION, CAPITOL RECORDS, LLC, ELEKTRA ENTERTAINMENT GROUP INC., LAFACE RECORDS LLC, SONY MUSIC ENTERTAINMENT, UMG RECORDINGS, INC., WARNER BROS. RECORDS INC., WARNER MUSIC GROUP CORP., and ZOMBA RECORDING LLC, *Plaintiffs*, v. VITA TKACH, and DOES 1-10, D/B/A GROOVESHARK.IO AND GROOVSHARK.PW *Defendants*.	CIVIL ACTION NO. 15-CV-03701-AJN

Declaration of Ólafur Guðmundsson in Support of Non-Party CloudFlare, Inc.'s Opposition to Plaintiff's Application for Supplemental Order

I, Ólafur Guðmundsson, declare and state as follows:

1. My name is Ólafur Guðmundsson. I have more than thirty years of professional experience in computer and network sciences, with extensive experience in network protocols and security. I hold an MS in Computer Science from the University of Maryland College Park (1987) and a BS in Computer Science from Háskóli Íslands (1983) in Iceland. One of my main areas of focus for the last two decades has been the Domain Name System ("DNS") and DNS security ("DNSSEC").

2. I have held Senior Network Scientist and CTO roles at various technology companies and DNS providers including Shinkuro, Inc., Binnacle Systems Inc., NeuStar, and Intel. In addition to my professional activities, I am one of the twenty-one TCRs (Trusted Community Representatives) selected from around the globe by the Internet Corporation for Assigned Names and Numbers (ICANN), the entity that oversees the Domain Name System. This position makes me a key officer for the DNS root key, meaning that I am one

of a handful of individuals who can enable a change to the DNS infrastructure, which powers the Internet. I have been a leading contributor to the Internet Engineering Task Force (IETF) in the specifications and operations of the DNS protocol, serving as a chair of the DNS protocol Working Group for a many years.

3. I am currently a Systems Engineer at CloudFlare, where I serve as the company's "DNS guru," working on enhancing the DNS services, deploying DNSSEC and improving DNS systems in general. One of my tasks is to modernize DNS registration systems globally.

The Role of the Domain Name Registry and Domain Name Registrars

4. The simplest way to explain DNS is that it is a telephone book for the Internet. When a user requests a site by a domain name, like www.example.com, the DNS system translates the request into an Internet Protocol (IP) address, like 93.184.216.119. DNS is designed to be a distributed and reliable system that keeps working even when there are failures. The main protocol element that matters is the DNS recursive resolver, which does the work of finding the information on behalf of a requesting application. DNS is a replicated distributed database system. It is in a sub-class called "loosely coherent." What this means is, first, there are many "sources" for answers, and second, the answers may differ during a transition, third, answers are cached for a specified time by resolvers, and fourth, the state of the resolver before it gets a query affects the answer returned to the browser.

5. A domain name registry is an organization which maintains a list of domain names and the associated registrant info for a top level domain (TLD).

6. A domain name registrar is a corporation authorized by a registry to sell access to domain names for a given TLD. The registrar is ultimately in control of what a user who navigates to a specific domain name sees.

7. Taking down a domain, such as in response to a court order, follows a well-established process in the Internet industry. Those takedowns must happen at the website's origin host(s) or at the registrar. A takedown at those places is far more effective at removing the infringing content from the Internet. A takedown from a hosting provider or providers would in fact remove the content from the Internet. A removal by a registrar would also make a site inaccessible ("go dark") at a particular domain name.

8. While it is possible that a website owner might create a wholly new Internet presence when its domain name is deactivated, they could not continue to make data available to visitors using the same domain name if a registrar deactivates the name.

CloudFlare Background and How CloudFlare Works

9. CloudFlare's network operates out of 34 data centers in 25 countries on all 6 inhabited continents. The network functions as a "reverse proxy" and automatically optimizes the delivery of CloudFlare customers' websites from their hosting server to their clients' browsers. This gives visitors to a website faster page load times and better performance, while blocking threats and abusive bots and crawlers from attacking the websites.

10. A typical CloudFlare customer has pointed their domain name settings to CloudFlare's nameservers. The term for this is "delegating DNS to CloudFlare." This change is configured via the customer's DNS registrar, outside of the CloudFlare network. CloudFlare is *not* a DNS registrar *nor* a DNS registry for its customers.

11. An authoritative DNS provider is an entity which can return the original and definitive answers to DNS queries such as the IP address of a mail server or website.

12. CloudFlare becomes the authoritative DNS provider for its customers when three factors are present. First, the customer must create and activate a valid CloudFlare account. Second, the customer must populate its DNS information in CloudFlare's customer database. Third, through its registrar or registry provider, the customer must point its DNS settings at the nameservers assigned to it by CloudFlare. This last factor occurs outside of CloudFlare's infrastructure completely. CloudFlare is then able to proxy requests for the customer's website.

13. While CloudFlare provides authoritative DNS for its customers who have met these factors, the term "authoritative" does not mean that CloudFlare has control over DNS content for the customer. Unlike registering a domain name, which requires a registrar, a website does not need to rely on a third party for authoritative DNS. Authoritative DNS servers are cheap, plentiful, and easily available to a website from thousands of providers around the world. Anyone can operate their own authoritative DNS server, and many do. Any website owner can point its DNS settings at or away from CloudFlare's nameservers. The customer's settings can be pointed, on the fly, to another provider's nameservers or directly at the customer's own nameservers for all or part of the website's traffic.

14. While CloudFlare's service makes use of and is provisioned through DNS, CloudFlare does not control the configuration of a customer's domain name – only the customer does.

15. Once DNS is properly configured, the CloudFlare network is a passive conduit for its customers' content, merely transmitting customer data from the customer's origin server to the customers' clients. CloudFlare has no control over the contents of a site.

16. CDN and reverse proxy services are a value-add but they are not necessary to the operation of a website. Any website can serve its own requests from one or more physical locations. Removing a website from the CloudFlare network (or, indeed, preventing a website from obtaining CDN and reverse proxy services entirely, from any provider) would not remove the content from the Internet. Rather, doing so may simply slow that website's performance and make the website more vulnerable to malicious attack.

What Happens when CloudFlare Removes a Customer

17. As mentioned above, CloudFlare cannot make a website or its content unavailable by ceasing to service a customer.

18. Since the customer's DNS delegation settings occur outside of the CloudFlare network, there are two processes by which CloudFlare can remove the customer from its network. The first is to simply have CloudFlare nameservers return the customer's origin server's IP addresses. This process, called FINTing (for "Failed INTernal"), routes traffic around the CloudFlare network directly to the customer's origin servers. Content does not disappear from the Internet, nor is it unavailable for more than a vanishingly small period of time, if at all.

19. The second process is to completely deconfigure any DNS response to a DNS query relating to the customer's website. Such a process will return a REFUSED response to any DNS query for the customers DNS names. When the DNS recursive resolver, which acts on behalf of a web browser, receives the REFUSED message from all of the authoritative DNS servers it returns a SERVFAIL message back to the browser. When presented with a SERVFAIL, the web surfer's browser will not be able to find the customer's website. The customer can detect this change immediately. If a REFUSED response is returned from CloudFlare's DNS resolvers, the customer need only restore its DNS settings to use its own nameservers instead of CloudFlare's.

20. In order to understand how long it takes for a customer to restore service, it is important to understand the nature of DNS. Different DNS resolvers employ different strategies to find the best information. Resolvers go out of their way to overcome failures in the system and answer as quickly as possible. When a customer changes DNS operators, like when it is removed from CloudFlare's system, this changes the set of DNS servers that queries will be sent to. Because of DNS's distributed nature, there is no explicit time

at which the customer has "restored service." Rather, there is a short time period where *some* browsers may not be able to reach the site.

I swear under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Date: May 28, 2015

Ólafur Gud

Ólafur Guðmundsson

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the CM/ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants.

/s/ William J. Harrington